

**UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS**

NATHAN SILVA, Derivatively on Behalf of
Nominal Defendant CROWDSTRIKE
HOLDINGS, INC.,

Plaintiff,

v.

GERHARD WATZINGER, GEORGE
KURTZ, ROXANNE AUSTIN, CARY
DAVIS, JOHANNA FLOWER, SAMEER
GANDHI, DENIS O'LEARY, LAURA
SCHUMACHER, GODFREY SULLIVAN,
MICHAEL SENTONAS, and BURT
PODBERE,

Defendants,

and

CROWDSTRIKE HOLDINGS, INC.,

Nominal Defendant.

VERIFIED SHAREHOLDER DERIVATIVE COMPLAINT

Plaintiff Nathan Silva (“Plaintiff”), by and through his undersigned attorneys, brings this derivative complaint for the benefit of nominal defendant CrowdStrike Holdings, Inc. (“CrowdStrike” or the “Company”), against its Board of Directors (the “Board”) and certain of its executive officers seeking to remedy Defendants’ (defined below) breaches of fiduciary duties and violations of federal law. Plaintiff alleges the following based upon personal knowledge as to himself and his own acts, and information and belief as to all other matters, based upon, *inter alia*, the investigation conducted by and through Plaintiff’s attorneys, which included, among other things, a review of Defendants’ publicly available documents, conference call transcripts and announcements made by Defendants, United States Securities and Exchange

Commission (“SEC”) filings, press releases published by and regarding CrowdStrike, legal filings, news reports, securities analysts’ reports about the Company, the securities class action captioned *Plymouth Cnty. Ret. Ass’n v. CrowdStrike Holdings, Inc.*, 1:24-cv-00857-RP (W.D. Tex.) (the “Securities Class Action”), and other publicly available information.

NATURE OF THE ACTION

1. This is a shareholder derivative action brought by Plaintiff on behalf of CrowdStrike against certain of its officers and members of the Company’s Board of Directors (the “Individual Defendants”)¹ for breaches of their fiduciary duties from at least November 29, 2023 through July 29, 2024 (the “Relevant Period”), as set forth below.

2. According to the Company’s public filings, CrowdStrike is a “global cybersecurity leader” that has “redefined modern security with the world’s most advanced cloud-native platform for protecting critical areas of enterprise risk.” The Company’s primary focus is on developing platforms to stop cybersecurity breaches.

3. The Company’s main proprietary platform is CrowdStrike Falcon XDR (“Falcon”), which the Company describes as “the definitive platform for cybersecurity consolidation, purpose-built to stop breaches.” The Falcon platform purportedly uses artificial intelligence (“AI”) to detect, prevent, and respond to security breach threats.

4. As detailed herein, throughout the Relevant Period, the Individual Defendants misrepresented the efficacy of Falcon, continuously assuring investors that the Company’s technology was “validated, tested, and certified,” and that any potential risks involving the

¹ The Individual Defendants are Gerhard Watzinger (“Watzinger”), George Kurtz (“Kurtz”), Cary Davis (“Davis”), Johanna Flower (“Flower”), Sammer Gandhi (“Gandhi”), Denis O’Leary (“O’Leary”), Laura Schumacher (“Schumacher”), Godfrey Sullivan (“Sullivan”), Michael Sentonas (“Sentonas”), and Burt Podbere (“Podbere”). “Defendants” means CrowdStrike and the Individual Defendants.

development of the platform were merely hypothetical. However, in reality, as was known by the Individual Defendants, the Company failed to adequately develop, test, and deploy updates to the Falcon program, making Falcon susceptible to errors.

5. The truth began to emerge on July 19, 2024 when, shortly after midnight, CrowdStrike released an update to the Falcon platform, which caused technology outages to customers that affected millions of users of Microsoft Windows systems worldwide. The outage impacted approximately 8.5 million devices worldwide, but hit the healthcare, banking, and airline sectors the hardest.²

6. On the news of the outage, the Company's stock price fell \$38.09 per share, or approximately 11.1%, to close at \$304.96 per share on July 19, 2024.

7. The truth continued to emerge on July 22, 2024, when: (i) it was revealed that Defendant Kurtz was contacted by Congress to testify regarding the CrowdStrike Outage;³ (ii) analysts, including Guggenheim Securities and BTIG, downgraded CrowdStrike's stock rating;⁴ and (iii) *Forbes* published an article revealing that the devastating effects that the CrowdStrike outage caused airlines were continuing to plague many airlines, mainly Delta Air Lines.⁵

8. On this news, the Company's stock price fell \$41.05 per share, or approximately 13.46%, to close at \$263.91 per share on July 22, 2024.

9. Then, on July 29, 2024, the truth fully emerged when it was revealed that Delta Air

² Brian Fung, *We Finally Know What Caused the Global Tech Outage – and How Much It Cost*, CNN (Jul. 24, 2024), <https://www.cnn.com/2024/07/24/tech/crowdstrike-outage-cost-cause/index.html>.

³ Kanishka Singh, *US Congressional Panel Calls on CrowdStrike CEO to Testify on Outage*, REUTERS (Jul. 22, 2024), <https://www.reuters.com/technology/cybersecurity/us-house-panel-calls-crowdstrike-ceo-testify-outage-washington-post-reports-2024-07-22/>.

⁴ Jordan Novet, *CrowdStrike Shares Tumble as Fallout from Global Tech Outage Continues*, CNBC (Jul. 22, 2024), <https://www.cnbc.com/2024/07/22/crowdstrike-shares-tumble-as-fallout-from-global-tech-outage-continues.html>; George Maybach, *BTIG Downgrades CrowdStrike Holdings (CRWD)*, FINTEL (Jul. 23, 2023), <https://news.fintel.io/news/btig-downgrades-crowdstrike-holdings-crwd-412>.

⁵ Geoff Whitmore, *The CrowdStrike Outage is Still Impacting Airlines*, FORBES (Jul. 22, 2024), <https://www.forbes.com/sites/geoffwhitmore/2024/07/22/the-crowdstrike-outage-is-still-impacting-airlines/>.

Lines hired a prominent attorney, David Boies, to pursue potential damages from CrowdStrike and Microsoft for the outage.⁶

10. On this news, the Company's stock price fell \$25.16 per share, or approximately 9.72%, to close at \$233.65 per share on July 30, 2024.

11. As set forth herein, the Individual Defendants breached their fiduciary duties by issuing, causing the issuance of, and/or failing to correct the materially false and/or misleading statements and omissions of material fact to the investing public. Specifically, the Individual Defendants failed to disclose to investors that: (i) the Company had insufficient controls in place concerning the procedures used by the Company to update the Falcon program; (ii) the Company was not properly testing updates to the Falcon platform prior to rolling the updates out to CrowdStrike's customers; (iii) the inadequate software testing created a substantial risk that an update to the Falcon platform could result in widespread technology outages; (iv) any such outages caused by the updates would cause substantial reputational harm and legal risk to the Company; and (v) as a result of the foregoing, Defendants' positive statements about the Company's business, operations, and prospects were materially misleading and/or lacked a reasonable basis.

12. As a result of the foregoing, the Securities Class Action was filed against the Company and Defendants Kurtz and Podbere on July 30, 2024, in the United States District Court for the Western District of Texas.

13. Furthermore, two consumer class action lawsuits, captioned *Del Rio v. CrowdStrike Holdings, Inc.*, 1:24-cv-00881-RP (W.D. Tex.) and *Harlan v. CrowdStrike Holdings, Inc.*, 1:24-cv-00954-RP (W.D. Tex.), were filed against the Company in connection with the outage on

⁶ Jordan Novet & Ari Levy, *Delta Hires David Boies to Seek Damages from CrowdStrike, Microsoft After Outage*, CNBC (Jul. 29, 2024), <https://www.cnbc.com/2024/07/29/delta-hires-david-boies-to-seek-damages-from-crowdstrike-microsoft-.html>.

August 5, 2024 and August 19, 2024, respectively, in the United States District Court for the Western District of Texas (collectively, the “Consumer Class Actions”).

14. As a direct and proximate result of the Individual Defendants’ misconduct, the Company has incurred significant financial losses, including the cost of defending and paying class-wide damages in the Securities Class Action and the Consumer Class Actions, as well as additional losses, including reputational harm and loss of goodwill.

15. Moreover, in light of the breaches of fiduciary duty engaged in by the Individual Defendants, most of whom are the Company’s current directors, their collective engagement in fraud, the substantial likelihood of the directors’ liability in this derivative action and Defendants’ liability in the Securities Class Action, their being beholden to each other, their longstanding business and personal relationships with each other, and their not being disinterested and/or independent directors, a majority of CrowdStrike’s Board cannot consider a demand to commence litigation against themselves and the other Individual Defendants on behalf of the Company with the requisite level of disinterestedness and independence. Accordingly, Plaintiff did not make a demand on the Board because, as further detailed herein, demand would be a futile and useless act.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331 and Section 27 of the Securities Exchange Act of 1934 (the “Exchange Act”) over the claims asserted herein for violations of Section 14(a) of the Exchange Act (15 U.S.C. §§ 78n(a) and Rule 14a-9 (17 C.F.R. §240.14a-9) promulgated thereunder by the SEC.

17. Plaintiff’s claims also raise a federal question pertaining to the claims made in the Securities Class Action based on violations of the Exchange Act.

18. This Court has supplemental jurisdiction over Plaintiff's state law claims pursuant to 28 U.S.C. § 1367(a).

19. This action is not a collusive action designed to confer jurisdiction on a court of the United States that it would not otherwise have.

20. In connection with the acts, conduct and other wrongs complained of herein, the Individual Defendants, directly or indirectly, used the means and instrumentalities of interstate commerce, the United States mail, and the facilities of a national securities market.

21. Venue is proper in this District pursuant to Section 27(a) of the Exchange Act and 28 U.S.C. §1391(b)(1), as CrowdStrike maintains its principal executive offices in this District and a substantial portion of the acts and omissions alleged herein, including the dissemination of materially false and misleading information, occurred in this District.

PARTIES

Plaintiff

22. Plaintiff is, and has been at all relevant times, a shareholder of CrowdStrike.

Nominal Defendant

23. Nominal Defendant CrowdStrike is a Delaware corporation with its principal executive offices located at 206 E. 9th Street, Suite 1400, Austin, Texas 78701. CrowdStrike's common stock trades on the NASDAQ under the ticker symbol "CRWD."

Individual Defendants

24. Defendant Watzinger has served as Chairman of the Board since April 2012. Watzinger also serves as a member of the Company's Audit Committee, Nominating and Corporate Governance Committee, and Transaction Committee. According to the Company's public filings, Defendant Watzinger received \$349,381 in compensation from the Company in 2023, and \$374,668 in 2024.

25. Defendant Kurtz is co-founder of the Company and has served as Chief Executive Officer (“CEO”) and President of the Company and as a member of the Board since November 2011. Kurtz also serves as a member of the Company’s Transaction Committee. According to the Company’s public filings, Defendant Kurtz received \$36,532,681 in compensation from the Company in 2023, and \$46,983,855 in 2024.

26. Defendant Austin has served as a member of the Board since September 2018. Austin also serves as Chair of the Company’s Audit Committee. According to the Company’s public filings, Defendant Austin received \$310,048 in compensation from the Company in 2023, and \$334,668 in 2024.

27. Defendant Davis has served as a member of the Board since July 2013. Davis also serves as a member of the Company’s Compensation Committee. According to the Company’s public filings, Defendant Davis received \$275,912 in compensation from the Company in 2023, and \$299,367 in 2024.

28. Defendant Flower has served as a member of the Board since January 2023. Flower previously served as the Company’s Chief Marketing Officer from November 2014 until August 2020 and from January 2022 until November 2022. According to the Company’s public filings, Defendant Flower received \$444,299 in compensation from the Company in 2023, and \$315,927 in 2024.

29. Defendant Gandhi has served as a member of the Board since August 2013. Gandhi also serves as Chair of the Company’s Compensation Committee and as a member of the Company’s Transaction Committee. According to the Company’s public filings, Defendant Gandhi received \$284,579 in compensation from the Company in 2023, and \$309,450 in 2024.

30. Defendant O’Leary has served as a member of the Board since December 2011.

O’Leary also serves as Chair of the Company’s Nominating and Corporate Governance Committee. According to the Company’s public filings, Defendant O’Leary received \$277,245 in compensation from the Company in 2023, and \$299,867 in 2024.

31. Defendant Schumacher has served as a member of the Board since November 2020. Schumacher also serves as a member of the Company’s Nominating and Corporate Governance Committee. According to the Company’s public filings, Defendant Schumacher received \$271,829 in compensation from the Company in 2023, and \$294,867 in 2024.

32. Defendant Sullivan has served as a member of the Board since December 2017. According to the Company’s public filings, Sullivan received \$277,245 in compensation from the Company in 2023, and \$299,867 in 2024.

33. Defendant Sentonas has served as President of the Company since March 2023. Sentonas previously served as the Company’s Vice President, Technology Strategy from May 2015 until February 2020 and as the Company’s Chief Technology Officer from February 2020 until March 2023. According to the Company’s public filings, Defendant Sentonas received \$35,648,591 in compensation from the Company in 2024.

34. Defendant Podbere has served as Chief Financial Officer (“CFO”) of the Company since September 2015. According to the Company’s public filings, Defendant Podbere received \$21,214,629 in compensation from the Company in 2023, and \$20,206,385 in 2024.

FIDUCIARY DUTIES OF THE INDIVIDUAL DEFENDANTS

35. By reason of their positions as officers and/or directors of CrowdStrike, and because of their ability to control the business and corporate affairs of CrowdStrike, the Individual Defendants owed CrowdStrike and its shareholders fiduciary obligations of trust, loyalty, good faith, and due care, and were and are required to use their utmost ability to control and manage

CrowdStrike in a fair, just, honest, and equitable manner. The Individual Defendants were and are required to act in furtherance of the best interests of CrowdStrike and its shareholders.

36. Each director and officer of the Company owes to CrowdStrike and its shareholders the fiduciary duty to exercise good faith and diligence in the administration of the Company and in the use and preservation of its property and assets and the highest obligation of fair dealing.

37. The Individual Defendants, because of their positions of control and authority as directors and/or officers of CrowdStrike, were able to and did, directly and/or indirectly, exercise control over the wrongful acts complained of herein.

38. To discharge their duties, the officers and directors of CrowdStrike were required to exercise reasonable and prudent supervision over the management, policies, controls, and operations of the Company.

39. Each Individual Defendant, by virtue of his or her position as a director and/or officer owed to the Company and to its shareholders the highest fiduciary duties of loyalty, good faith, and the exercise of due care and diligence in the management and administration of the affairs of the Company, as well as in the use and preservation of its property and assets. The conduct of the Individual Defendants complained of herein involves a knowing and culpable violation of their obligations as directors and/or officers of CrowdStrike, the absence of good faith on their part, or a reckless disregard for their duties to the Company and its shareholders that the Individual Defendants were aware or should have been aware posed a risk of serious injury to the Company.

40. As senior executive officers and directors of a publicly-traded company whose common stock was registered with the SEC pursuant to the Exchange Act and traded on the NASDAQ, the Individual Defendants had a duty to prevent and not to effect the dissemination of

inaccurate and untruthful information with respect to the Company's financial condition, performance, growth, financial statements, products, management, internal controls, earnings, and present and future business prospects, including the dissemination of false and/or materially misleading information regarding the Company's business, prospects, and operations, and had a duty to cause the Company to disclose in its regulatory filings with the SEC all those facts described in this Complaint that it failed to disclose, so that the market price of the Company's common stock would be based upon truthful, accurate, and fairly presented information.

41. To discharge their duties, the officers and directors of CrowdStrike were required to exercise reasonable and prudent supervision over the management, policies, practices, and internal controls of the Company. By virtue of such duties, the officers and directors of CrowdStrike were required to, among other things:

(i) Ensure that the Company was operated in a diligent, honest, and prudent manner in accordance with the laws and regulations of Delaware, Texas, and the United States, and pursuant to CrowdStrike's own Code of Business Conduct and Ethics (the "Code of Conduct");

(ii) Conduct the affairs of the Company in an efficient, business-like manner so as to make it possible to provide the highest quality performance of its business, to avoid wasting the Company's assets, and to maximize the value of the Company's stock;

(iii) Remain informed as to how CrowdStrike conducted its operations, and, upon receipt of notice or information of imprudent or unsound conditions or practices, to make reasonable inquiry in connection therewith, and to take steps to correct such conditions or practices;

(iv) Establish and maintain systematic and accurate records and reports of the business and internal affairs of CrowdStrike and procedures for the reporting of the business and internal affairs to the Board and to periodically investigate, or cause independent investigation to be made of, said reports and records;

(v) Maintain and implement an adequate and functioning system of internal legal, financial, and management controls, such that CrowdStrike's operations would comply with all applicable laws and CrowdStrike's financial statements and regulatory filings filed with the SEC and disseminated to the public and the Company's shareholders would be accurate;

(vi) Exercise reasonable control and supervision over the public statements made by the Company's officers and employees and any other reports or information that the Company was required by law to disseminate;

(vii) Refrain from unduly benefiting themselves and other Company insiders at the expense of the Company; and

(viii) Examine and evaluate any reports of examinations, audits, or other financial information concerning the financial affairs of the Company and to make full and accurate disclosure of all material facts concerning, *inter alia*, each of the subjects and duties set forth above.

42. Each of the Individual Defendants further owed to CrowdStrike and the shareholders the duty of loyalty requiring that each favor CrowdStrike's interest and that of its shareholders over their own while conducting the affairs of the Company and refrain from using their position, influence, or knowledge of the affairs of the Company to gain personal advantage.

43. At all times relevant hereto, the Individual Defendants were the agents of each other and of CrowdStrike and were at all times acting within the course and scope of such agency.

44. Because of their advisory, executive, managerial, and directorial positions with CrowdStrike, each of the Individual Defendants had access to adverse, non-public information about the Company.

45. The Individual Defendants, because of their positions of control and authority, were able to and did, directly or indirectly, exercise control over the wrongful acts complained of herein, as well as the contents of the various public statements issued by CrowdStrike.

CROWDSTRIKE'S CODE OF CONDUCT

46. The Company's Code of Conduct applies to all of the Company's "employees, officers, Board members and independent contractors."

47. In a section titled, "The Code and the Law," the Code of Conduct states, in relevant part, "Violations of laws, rules, and regulations may subject the violator to individual criminal or civil liability, as well as disciplinary action by CrowdStrike. . . .These violations may also subject CrowdStrike to civil or criminal liability or the loss of business."

48. In a section titled "Insider Trading," the Code of Conduct states, in relevant part:

Insider trading violates this Code and the law, and may result in substantial civil and criminal penalties, including the possibility of a jail sentence. . . .

Buying or selling stock while in possession of material non-public information or passing such information along to others so that they may buy or sell stock, constitutes illegal insider trading.

49. In a section titled "Financial Integrity, Records, and Accounting," the Code of Conduct states, in relevant part:

Making false or misleading records or documentation is strictly prohibited. . . .

All of CrowdStrike's books, records, accounts and financial statements must be:

- maintained in reasonable detail.

- must accurately, fairly, and completely reflect the transactions and matters to which they relate.
- must conform to applicable legal requirements and to CrowdStrike's system of internal controls.

CROWDSTRIKE'S AUDIT COMMITTEE CHARTER

50. CrowdStrike's Audit Committee Charter states that the purpose of the Audit Committee is to:

- assist the Board in its oversight of:
 - the integrity of the Company's financial statements and internal controls;
 - the qualifications, independence and performance of the Company's independent auditor;
 - the performance of the Company's internal audit function;
 - the Company's compliance with legal and regulatory requirements; and
- prepare the Committee report that the Securities and Exchange Commission (the "SEC") rules require to be included in the Company's annual proxy statement.

51. In a section titled "Responsibilities," the Audit Committee Charter states:

The basic responsibility of the members of the Committee is to exercise their business judgment to act in what they reasonably believe to be in the best interests of the Company and its shareholders. In discharging that obligation, members should be entitled to rely on the honesty and integrity of the Company's senior executives and its outside advisors and auditors, to the fullest extent permitted by law. In addition to any other responsibilities which may be assigned from time to time by the Board, the Committee is responsible for the following matters.

52. Also in the Responsibilities section of the Audit Committee Charter, a subsection titled "Independent Auditor," states that:

- The Committee shall be directly responsible for the appointment, compensation, retention, termination, and oversight of the work of any accounting firm engaged for the purpose of preparing or issuing an audit report or performing other audit, review or attest services for the Company (subject, if applicable, to shareholder ratification). Each such accounting firm shall report directly to the Committee.

- The Committee shall pre-approve the audit services and non-audit services (including the fees and terms thereof) to be provided by the Company's independent auditor pursuant to pre-approval policies and procedures established by the Committee, subject to the de minimis exception for non-audit services described in the Securities Exchange Act of 1934 that are approved by the Committee prior to the completion of the audit. The Committee may delegate its authority to pre-approve services to the Committee Chair, or one or more Committee members, provided that such designees present any such approvals to the full Committee at the next Committee meeting.
- The Committee shall discuss with the independent auditor its responsibilities under generally accepted auditing standards, review and approve the planned scope and timing of the independent auditor's annual audit plan(s) and discuss significant findings from the audit and any problems or difficulties encountered, including any restrictions on the scope of the auditor's activities or on access to requested information, and any significant disagreements with management.
- The Committee shall evaluate the independent auditor's qualifications, performance and independence, and shall present its conclusions with respect to the independent auditor to the full Board on at least an annual basis. As part of such evaluation, at least annually, the Committee shall:
 - obtain and review a report or reports from the Company's independent auditor:
 - describing the independent auditor's internal quality-control procedures;
 - describing any material issues raised by (i) the most recent internal quality-control review, peer review or Public Company Accounting Oversight Board ("PCAOB") review, of the independent auditing firm, or (ii) any inquiry or investigation by governmental or professional authorities, within the preceding five years, regarding one or more independent audits carried out by the auditing firm; and any steps taken to deal with any such issues; and
 - describing all relationships between the independent auditor and the Company consistent with applicable requirements of the PCAOB regarding the independent auditor's communications with the Committee concerning independence; • consider whether the provision of permitted non-audit services is compatible with maintaining the independent auditor's independence;
 - review and evaluate the lead audit partner of the independent auditor team(s), as well as other senior members;

- confirm and evaluate the rotation of the audit partners on the audit engagement team as required by law;
 - consider whether the independent auditor should be rotated, so as to assure continuing auditor independence; and
 - obtain the opinion of management and the Company personnel primarily responsible for the design and implementation of the internal audit function of the independent auditor's performance.
- The Committee shall establish policies for the Company's hiring of current or former employees of the independent auditor.

53. Under the same Responsibilities section, in a subsection titled "Financial Statements; Disclosure and Other Risk Management and Compliance Matters," the Audit Committee Charter states that:

- The Committee shall meet to review and discuss with management and the independent auditor the annual audited financial statements and unaudited quarterly financial statements, including reviewing the Company's specific disclosures under "Management's Discussion and Analysis of Financial Condition and Results of Operations," prior to the filing of the Company's Form 10-K or Form 10-Q with the SEC;
- The Committee shall review with management, the head of internal audit, and the independent auditor, whenever the Committee deems appropriate:
 - any analyses or other written communications prepared by management and/or the independent auditor setting forth significant financial reporting issues and judgments made in connection with the preparation of the financial statements, including analyses of the effects of alternative U.S. Generally Accepted Accounting Principles ("GAAP") methods on the financial statements;
 - the critical accounting policies and practices of the Company;
 - the effect of regulatory and accounting initiatives, as well as off-balance sheet transactions and structures, on the Company's financial statements; and
 - any major issues regarding accounting principles and financial statement presentations, including any significant changes in the Company's selection or application of accounting principles.

- The Committee, or the Chair of the Committee, shall review the Company's earnings press releases prior to public dissemination, the type and presentation of information included in the Company's earnings press releases, as well as financial information and earnings guidance provided to analysts and rating agencies, paying particular attention to the use of non-GAAP financial information.
- The Committee, or the Chair of the Committee, may review any of the Company's financial information and earnings guidance provided to analysts and ratings agencies and any of the Company's other financial disclosures, such as earnings press releases, as the Chair of the Committee deems appropriate.
- The Committee shall, in conjunction with the Chief Executive Officer and Chief Financial Officer of the Company, review the Company's disclosure controls and procedures and internal control over financial reporting. The review of internal control over financial reporting shall include whether there are any significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting which are reasonably likely to affect the Company's ability to record, process, summarize and report financial information and any fraud involving management or other employees with a significant role in internal control over financial reporting. The Committee shall also review any special audit steps adopted in light of material control deficiencies.
- The Committee shall review and discuss with the independent auditor and management any current accounting trends and developments, and take such action with respect thereto as may be deemed appropriate.
- The Committee shall review and discuss with the independent auditor any audit problems or difficulties and management's response thereto, including those matters required to be discussed with the Committee by the auditor pursuant to established auditing standards, as amended, such as:
 - any restrictions on the scope of the independent auditor's activities or on access to requested information;
 - any accounting adjustments that were noted or proposed by the auditor but were not adopted or reflected;
 - any communications between the audit team and the audit firm's national office regarding auditing or accounting issues presented by the engagement;
 - any management or internal control letter issued, or proposed to be issued, by the auditor; and

- any significant disagreements between management and the independent auditor.
- In connection with its oversight responsibilities, the Committee shall be directly responsible for the resolution of disagreements between management and the auditor regarding the Company's financial reporting.
- The Committee shall review the Company's policies and practices with respect to risk assessment and risk management, including the Company's policies and practices pertaining to financial accounting, investment, tax, and cybersecurity matters, and shall discuss with management the Company's major financial risk exposures and the steps that have been taken to monitor and control such exposures.
- The Committee shall establish procedures for:
 - the receipt, retention and treatment of complaints received by the Company regarding accounting, internal accounting controls or auditing matters, and
 - the confidential, anonymous submission by employees of the Company of concerns regarding questionable accounting or auditing matters.
- The Committee shall prepare the Committee report that the SEC rules require to be included in the Company's annual proxy statement.
- The Committee shall review the Company's compliance with laws and regulations, including major legal and regulatory initiatives. The Committee shall also review any major litigation or investigations against the Company that may have a material impact on the Company's financial statements. The Committee shall meet and discuss these matters with management and others as appropriate, including the General Counsel of the Company.

54. In the remainder of the Responsibilities section, the Audit Committee

Charter states that:

Internal Audit Function

- The Committee shall review any process of appointment and/or replacement of the Company's head of internal audit.
- At least annually, the Committee shall evaluate the responsibilities, budget, staffing, planned scope of work, and performance of the internal audit function. Such review shall include a review of the responsibilities, budget and staffing of the Company's internal audit function with the independent auditor.

- The Committee shall review any significant results of internal audits, recommendations prepared by the internal auditing department and management's responses thereto.

Reporting to the Board

- The Committee shall report to the Board periodically. This report shall include a review of any issues that arise with respect to the quality or integrity of the Company's financial statements, the Company's compliance with legal or regulatory requirements, the independence and performance of the Company's independent auditor, the performance of the internal audit function, and any other matters that the Committee deems appropriate or is requested to include by the Board.
- At least annually, the Committee shall evaluate its own performance and report to the Board on such evaluation.
- The Committee shall review and assess the adequacy of this charter annually and recommend any proposed changes to the Board.

Corporate Governance Matters

- The Committee may revise or amend the Policy for Reporting Concerns Related to Accounting, Auditing and Ethical Violations (Whistleblower Policy) as appropriate.
- The Committee shall review, and if appropriate, approve related party transactions in accordance with the Company's Related Person Transaction Policy.

Other Duties and Responsibilities

- The Committee will perform any other activities required by applicable law, rules or regulations, including those promulgated by the SEC and Nasdaq, and take such other actions and perform and carry out any other responsibilities and duties delegated to it by the Board or as the Committee deems necessary or appropriate consistent with its purpose.

SUBSTANTIVE ALLEGATIONS

Background

55. Founded in 2011, CrowdStrike is a cybersecurity company that purportedly “reinvented cybersecurity for the cloud era and transformed the way cybersecurity is delivered and

experienced by customers.” The Company’s primary customer base comes from large corporations from a variety of industries, including airlines, banks, and hospitals.

56. The Company’s primary business is the development of cybersecurity platforms to stop data breaches. The Company’s main cybersecurity platform is Falcon, which was designed to be the definitive platform for cybersecurity consolidation and built to stop breaches.

57. The Falcon platform is powered by the CrowdStrike Security Cloud and advanced AI. The platform’s single, lightweight agent collects and integrates data from across the enterprise, including endpoints, cloud workloads, identities, and third-party sources to train the Company’s AI to detect and prevent threats and drive workflow automation to give customers’ security teams an advantage to stop breaches.

58. The Company sells subscriptions to the Falcon platform and cloud modules to organizations across multiple industries, with the substantial majority of customers purchasing subscriptions with a term of one year.

59. According to the Company’s public filings, as of January 31, 2024, the Falcon platform had 29,000 customers, which was an increase of 26% from the following year.

The CrowdStrike Outage

60. As detailed herein, the technology outage was caused by a faulty update to CrowdStrike’s Falcon platform on July 19, 2024.

61. The Falcon platform uses on-sensor AI and machine learning models, which are kept up-to-date and strengthened with learnings from the latest threat telemetry from the sensor. Each sensor correlates context from its local graph store and live system activity into behaviors and indicators of attack in an ongoing process of refinement through a Sensor Detection Engine that combines built-in Sensor Content with Rapid Response Content from the cloud. The Rapid

Response Content is used to gather telemetry, identify indicators of adversary behavior, and augment novel detections and preventions on the sensor. Rapid Response Content is then delivered through Channel Files and interpreted by the sensor's Content Interpreter. Each Rapid Response Content is associated with a specific Template Type built into a sensor release, which provides the Content Interpreter with activity data and graph context to be matched against the Rapid Response Content.⁷

62. In February 2024, CrowdStrike introduced a new Template Type to the Falcon program to enable visibility into possible novel attack techniques that may affect certain Microsoft Windows mechanisms.⁸ This created a pre-defined set of fields to gather data, with the data then being delivered as Rapid Response Content to sensors via a corresponding Channel File numbered 291. The new Template Type update defined twenty input parameter fields, but the integration code associated with Channel File 291 supplied only twenty values to match against.⁹

63. Between March and April 2024, there were four updates deployed to the Rapid Response Content for Channel File 291, which were done without issue.¹⁰ This was because during the testing there was "wildcard matching criteria" added to the twenty-first input.¹¹

64. Shortly after midnight on July 19, 2024, the Company distributed another update to the Rapid Response Content for Channel File 291. However, the update was flawed. The new update required the sensor to inspect the twenty-first input parameter field, which was not the case in the previous testing.¹²

⁷ CrowdStrike, *External Root Cause Analysis – Channel File 291* (Aug. 6, 2024), <chrome-extension://efaidnbmnnnibpcjppcglefndmkaj/https://www.crowdstrike.com/wp-content/uploads/2024/08/Channel-File-291-Incident-Root-Cause-Analysis-08.06.2024.pdf>.

⁸ *Id.*

⁹ *Id.*

¹⁰ CrowdStrike, *Remediation and Guidance Hub: Channel 291 Incident* (last updated Aug. 6, 2024), <https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/>

¹¹ CrowdStrike, *supra* note 7.

¹² *Id.*

65. As a result of the update, a widespread technology outage occurred, which affected an estimated 8.5 million Windows devices. Although the Company pulled the update to Falcon just over an hour after it was released, the outage had already affected many customers, with a number of Windows systems having encountered “an endless reboot loop and the blue screen of death.”¹³

66. The health care, banking, and airline sectors were hit the hardest by the outage.¹⁴

67. Even days after the outage, commercial airlines were still grappling with the effects of the outage.¹⁵ In the four days following the outage, Delta Air Lines canceled more than 7,000 flights.¹⁶ Airlines, like Delta Air Lines, were suffering the consequences of the outage hardest days after because the system reboot that has to take place to coordinate new flights is complex, and the greater the number of flight disruptions, the harder it is to reset the system.¹⁷

68. The outage caused by CrowdStrike cost the Company’s customers millions of dollars in losses. As just one example, Delta Air Lines alleges that the outage cost Delta Air Lines \$550 million, with \$380 in lost revenue to due to refunding customers for flight costs and reimbursing customers, and \$170 million spent on other recovery expenses.¹⁸

The Company Knew, or Should Have Known of the Risks of its Software Updates of Falcon

69. During the Relevant Period, the Individual Defendants knew, or should have known, that the Company did not have the proper procedures in place for software update

¹³ Matt Kapko, *CrowdStrike Says Flawed Update Was Live for 78 Minutes*, CYBER SECURITY DIVE (Jul. 23, 2024), <https://www.cybersecuritydive.com/news/crowdstrike-flawed-update-78-minutes/722070/>.

¹⁴ Fung, *supra* note 2.

¹⁵ *Id.*

¹⁶ Elisabeth Buchwald, *Delta is Finally Emerging from Chaos. Did it Not Learn Anything from Southwest’s Meltdown?*, CNN (Jul. 24, 2024), <https://www.cnn.com/2024/07/24/business/delta-lessons-from-southwest-meltdown/index.html>.

¹⁷ *Id.*

¹⁸ Hope King et al., *Delta to Seek “At Least \$500 Million” From CrowdStrike and Microsoft*, AXIOS (Aug. 8, 2024), <https://www.axios.com/2024/08/08/delta-crowdstrike-outage-cost-550-million>.

development, testing, and deployment. The lack of proper procedures put the Company at risk of publishing software updates that contained flaws, invalid data, or errors, which is what ultimately occurred on July 19, 2024.

70. Indeed, experts in the technology and cybersecurity sphere spoke out about the proper procedures for software updates following the outage, scrutinizing the methods used by CrowdStrike for the Falcon update. For example, in an article published on July 19, 2024, Costin Raiu, who worked at Kaspersky, a Russian security software firm, for twenty-three years and led its threat intelligence team, commented on the potential flaws in CrowdStrike's update. The article stated, in relevant part:

During his years at Kaspersky, Raiu says, driver updates for Windows software were closely scrutinized and tested for weeks before they were pushed out. In this case, he suggests the configuration file may have been a far less scrutinized update that nonetheless able to change the way the kernel driver functioned and thus cause the crash.¹⁹

71. Additionally, in an article published on July 20, 2024, two cybersecurity experts commented on the methods used by CrowdStrike in the Falcon updates. Eric O'Neill, a former FBI counterterrorism and counterintelligence operative and cybersecurity expert, stated that "[w]hat Crowdstrike was doing was rolling out its updates to everyone at once. That is not the best idea. Send it to one group and test it. There are levels of quality control it should go through."²⁰ Peter Avery, vice president of security and compliance at Visual Edge IT, commented that the Company needs more safeguards in place to prevent future incidents and stated that "[the update] should have been tested in sandboxes, in many environments before it went out."²¹

¹⁹ Lily Hay Newman et al., *How One Bad CrowdStrike Update Crashed the World's Computers*, WIRED (Jul. 19, 2024), <https://www.wired.com/story/crowdstrike-outage-update-windows/>.

²⁰ Kevin Williams, *The CrowdStrike Fail and Next Global IT Meltdown Already in the Making*, CNBC (Jul. 20, 2024), <https://www.cnbc.com/2024/07/20/the-crowdstrike-fail-and-next-global-it-meltdown-already-in-the-making.html>.

²¹ *Id.*

72. Furthermore, in the report issued by the Company following the outage, CrowdStrike itself acknowledged that the testing for the Falcon update should have been conducted in a rollout, rather than releasing the update to all customers at once. In a section titled “Findings and Mitigations,” CrowdStrike stated that “[e]ach Template Instance should be deployed in a staged rollout” and that “[s]tagged development mitigates impact if a new Template Instance causes failures such as system crashes. . . .”²²

73. As detailed herein, despite the fact that proper update practices were known across the cybersecurity industry, and were acknowledged by the Company following the outage, the Individual Defendants made numerous materially false and misleading statements throughout the Relevant Period regarding the efficacy of the Falcon platform and the Company’s technology practices.

Individual Defendants’ Materially False and Misleading Statements

74. Throughout the Relevant Period, the Individual Defendants continuously published public documents touting the functionality of the Falcon platform and assured investors that CrowdStrike’s technology was “validated, tested, and certified.” However, the reality was that the Company had failed to adequately develop, test, and implement updates to the Falcon platform, making the platform susceptible to errors.

75. On November 28, 2023, the Company issued a press release announcing its financial results for the third quarter of the fiscal year 2024. In connection with the announcement, on November 29, 2023, CrowdStrike hosted an earnings call (the “Q3 2024 Earnings Call”), in which Defendant Kurtz touted the Falcon platform:

The drumbeat of innovation was loud and clear with multiple releases and announcements, showcasing CrowdStrike as the XDR leader, including the Falcon platform Raptor release, which standardizes all of our customers on LogScale.

²² CrowdStrike, *supra* note 7.

This builds our platform data gravity, coupling native Falcon data with third-party data ingest, further enabling our customers to realize SIEM and XDR use cases on Falcon. Falcon for IT, a new module to unify IT and tech ops. From hygiene to patching, Falcon for IT lets customers consolidate multiple use cases and replace legacy products with our single-agent architecture. Our new Falcon Data Protection module that liberates customers from legacy DLP products with modern, frictionless data security, which prevents data exfiltration.

Falcon Foundry, a no-code application development solution, enabling both customers and technology partners to build directly on Falcon. Foundry epitomizes the true definition of a platform offering limitless apps. We announced the acquisition of Bionic, bringing application security posture management to the Falcon Cloud Security suite. Falcon Cloud Security is the industry's most comprehensive and innovative cloud security offering, with integrated agent and agentless CSPM, CIEM, CWP, and now ASPM.

We released the beta and pricing for Charlotte AI, our AI-powered SOC analyst, which was incredibly well received. CrowdStrike's generative AI leveraging multiple foundational models can turn hours of work into minutes while democratizing cybersecurity, unlocking value and adoption across the entire breadth of the Falcon platform. Enthusiasm for Falcon for IT, our automation and hygiene module for IT teams, is exciting to witness because it is something so intuitive that our customers want. Like Data Protection, Falcon for IT solves a clear and long-neglected pain point where customers are forced to rely on multiple legacy products that have long outstayed their welcome.

Customers are eager to consolidate their aging estate while reducing cost and complexity. Falcon for IT illustrates the power of CrowdStrike's single-platform approach. We have the real estate and data foundation to solve ever-evolving use cases, delighting our customers while disrupting vendors that have failed to evolve. The resounding takeaway from my customer engagements at Fal.Con and throughout the quarter is that CrowdStrike is the right choice for CSOs, CIOs, executive teams, and boards.

76. Also in the Q3 2024 Earnings Call, Defendant Kurtz highlighted CrowdStrike's technology and efficacy, stating, in relevant part:

Across industry analyst firms, CrowdStrike is consistently top-rated. In Q3, CrowdStrike was awarded a perfect 100% across protection, visibility, and analytic detections in MITRE's latest ATT&CK testing, an industry first; recognized as Gartner Customers' Choice and one of the highest rated in their latest peer insights voice of the customer for EPP report; named a leader in the Forrester Wave for Endpoint Security; and positioned as a leader in the IDC Vulnerability Management Marketscape.

77. On the same day, November 29, 2023, the Company filed its quarterly report for the period ended October 31, 2023 on a Form 10-Q with the SEC (the “Q3 2024 10-Q”). In the Q3 2024 10-Q, the Company highlighted errors that could occur with the Falcon platform and harm CrowdStrike, framing them as merely hypothetical, stating, in relevant part:

We rely on third-party data centers, such as Amazon Web Services, and our own colocation data centers to host and operate our Falcon platform, and any disruption of or interference with our use of these facilities may negatively affect our ability to maintain the performance and reliability of our Falcon platform which could cause our business to suffer.

Our customers depend on the continuous availability of our Falcon platform. We currently host our Falcon platform and serve our customers using a mix of third-party data centers, primarily Amazon Web Services, Inc., or AWS, and our data centers, hosted in colocation facilities. Consequently, we may be subject to service disruptions as well as failures to provide adequate support for reasons that are outside of our direct control. We have experienced, and expect that in the future we may experience interruptions, delays and outages in service and availability from time to time due to a variety of factors, including infrastructure changes, human or software errors, website hosting disruptions and capacity constraints.

The following factors, many of which are beyond our control, can affect the delivery, availability, and the performance of our Falcon platform. . . .

- failure by us to maintain and update our cloud infrastructure to meet our data capacity requirements;
- errors, defects or performance problems in our software, including third-party software incorporated in our software;
- improper deployment or configuration of our solutions;
- the failure of our redundancy systems, in the event of a service disruption at one of our data centers, to provide failover to other data centers in our data center network; and
- the failure of our disaster recovery and business continuity arrangements.

The adverse effects of any service interruptions on our reputation, results of operations, and financial condition may be disproportionately heightened due to the nature of our business and the fact that our customers have a low tolerance for interruptions of any duration. Interruptions or failures in our service delivery could

result in a cyberattack or other security threat to one of our customers during such periods of interruption or failure. Additionally, interruptions or failures in our service could cause customers to terminate their subscriptions with us, adversely affect our renewal rates, and harm our ability to attract new customers. Our business would also be harmed if our customers believe that a cloud-based SaaS-delivered endpoint security solution is unreliable. While we do not consider them to have been material, we have experienced, and may in the future experience, service interruptions and other performance problems due to a variety of factors. The occurrence of any of these factors, or if we are unable to rapidly and cost-effectively fix such errors or other problems that may be identified, could damage our reputation, negatively affect our relationship with our customers or otherwise harm our business, results of operations and financial condition.

78. The Q3 2024 10-Q went on to highlight that failure to improve the Falcon program “could” impair the Company’s business, stating, in relevant part:

Our future success will depend in part on our ability to manage our growth effectively, which will require us to, among other things. . . . further improve our Falcon platform, including our cloud modules, and IT infrastructure, including expanding and optimizing our data centers, to support our business needs. . . . If we fail to achieve these objectives effectively, our ability to manage our expected growth, ensure uninterrupted operation of our Falcon platform and key business systems, and comply with the rules and regulations applicable to our business could be impaired.

79. The Q3 2024 10-Q was accompanied by certifications made by Defendants Kurtz and Podbere pursuant to Exchange Act Rule 13a-14(a) and Section 302 of the Sarbanes-Oxley Act of 2002 (the “SOX Certifications”). In the SOX Certifications, Defendants Kurtz and Podbere attested to the accuracy of the Q3 2024 10-Q.

80. On March 5, 2024, the Company issued a press release announcing its financial results for the fourth quarter and fiscal year 2024. In conjunction with the press release, CrowdStrike held an earnings call (the “Q4 2024 Earnings Call”). In the Q4 2024 Earnings Call, Defendant Kurtz again touted the Company’s technology, and the Falcon program specifically, stating, in relevant part:

Building on my founding vision, CrowdStrike is the only single-platform, single-agent technology in cybersecurity that solves use cases well beyond endpoint

protection. Falcon is the easiest and fastest cybersecurity technology to deploy. And our single AI-native platform makes vendor consolidation instant, frictionless, and natural. The feedback we receive from customers, prospects, and partners alike is consistent: eagerness to deploy the Falcon platform, ease of adopting more Falcon platform modules, and excitement from continuous innovation with new Falcon capabilities delivered weekly.

81. Importantly, in the Q4 2024 Earnings Call, Defendant Kurtz emphasized that “[t]he Falcon platform is validated, tested, and certified” and that “[i]ndustry analysts regularly recognize Falcon and our leadership.”

82. Shortly after the Q4 2024 Earnings Call, on March 7, 2024, the Company filed its annual report for the fiscal year ended January 31, 2024 on a Form 10-K with the SEC (the “2024 10-K”). The 2024 10-K boasted about CrowdStrike’s business model and the Falcon platform, stating, in relevant part:

We offer our customers compelling business value that includes ease of adoption, rapid time-to-value, superior efficacy rates in detecting threats and preventing breaches, and reduced total cost of ownership by consolidating legacy, siloed, and multi-agent security products in a single solution. We also allow thinly-stretched security organizations to automate previously manual tasks, freeing them to focus on their most important objectives. With the Falcon platform, organizations can transform how they combat threats, transforming from slow, manual, and reactionary to fast, automated, and predictive, while gaining visibility across the threat lifecycle.

Key benefits of our approach and the CrowdStrike Falcon platform include:

- **The Power of the Crowd:** Our crowdsourced data enables every customer to benefit from contributing to the Security Cloud. As more high fidelity data is fed into our Security Cloud, our AI models continue to train and improve, increasing the overall efficacy of the Falcon platform. This unique data layer is powered and turned into action by three complementary graph databases (Threat Graph, Asset Graph, and Intel Graph) to put threats, adversaries, and assets into the context needed to make the rapid, informed decisions that stop breaches.
- **High Efficacy, Low False Positives:** The vast telemetry of the Security Cloud and the best practices employed in continually training our AI models results in industry-leading efficacy rates and low false positives.

- **Consolidation of Siloed Products:** Integrating and maintaining numerous security products creates blind spots that attackers can exploit, is costly to maintain and negatively impacts user performance. Our cloud-native platform approach gives customers a unified approach to address their most critical areas of risk seamlessly. We empower customers to rapidly deploy and scale industry leading technologies across endpoint detection and response (“EDR”) and Extended Detection and Response (“XDR”), Identity Threat Protection, Threat Intelligence, Exposure Management, Cloud Security, Application Security Posture Management, Next-Generation SIEM and Modern Log Management, and IT Automation from a single platform.

- **Reducing Agent Bloat:** Our single intelligent lightweight agent enables frictionless deployment of our platform at scale, enabling customers to rapidly adopt our technology across any type of workload running on a variety of endpoints. The agent is non-intrusive to the end user, requires no reboots and continues to protect the endpoint and track activity even when offline. Through our single lightweight agent approach, customers can adopt multiple platform modules to address their critical areas of risk without burdening the endpoint with multiple agents. Legacy approaches often require multiple agents as they layer on new capabilities. This can severely impact user performance and create barriers to security.

- **Rapid Time to Value:** Our cloud-native platform was built to rapidly scale industry leading protection across the entire enterprise, eliminating lengthy implementation periods and professional services engagements that next-gen and legacy competitors may require. Our single agent, collect once and re-use many times approach enables us to activate new modules in real time.

- **Elite Security Teams as a Force Multiplier:** As adversaries continue to employ sophisticated malwareless attacks that exploit user credentials and identities, automation and autonomous security are no longer sufficient on their own. Stopping today’s sophisticated attacks requires a combination of powerful automation and elite threat hunting. Falcon Complete provides a comprehensive monitoring, management, response, and remediation solution to our customers and is designed to bring enterprise level security to companies that may lack enterprise level resources. CrowdStrike Falcon OverWatch, part of CrowdStrike Counter Adversary Operations, combines world-class human intelligence from our elite security experts with the power of the Falcon platform. OverWatch is a force multiplier that extends the capabilities and improves the productivity of our customers’ security teams. Because our world-class team can see attacks across our entire customer base, their expertise is enhanced by their constant visibility into the threat landscape. Additionally, the insights of our OverWatch team can then be leveraged by the Falcon platform to further enhance its autonomous capabilities, creating a positive feedback loop for our customers.

- **Alleviating the Skills Shortage through Automation:** CrowdStrike automates manual tasks to free security teams to focus on their most important job – stopping the breach. Our Falcon Fusion capability automates workflows to reduce the need to switch between different security tools and tasks, while our Falcon Insight XDR module provides a unified solution that enables security teams to rapidly and efficiently identify, hunt, and eliminate threats across multiple security domains using first and third party datasets.

- **Lower Total Cost of Ownership:** Our cloud-native platform eliminates our customers' need for initial or ongoing purchases of hardware and does not require their personnel to configure, implement or integrate disparate point products. Additionally, our comprehensive platform reduces overall personnel costs associated with ongoing maintenance, as well as the need for software patches and upgrades for separate products.

83. The 2024 10-K also discussed “potential” risks to the Falcon platform, stating, in relevant part:

We rely on third-party data centers, such as Amazon Web Services, and our own colocation data centers to host and operate our Falcon platform, and any disruption of or interference with our use of these facilities may negatively affect our ability to maintain the performance and reliability of our Falcon platform which could cause our business to suffer.

Our customers depend on the continuous availability of our Falcon platform. We currently host our Falcon platform and serve our customers using a mix of third-party data centers, primarily Amazon Web Services, Inc., or AWS, and our data centers, hosted in colocation facilities. Consequently, we may be subject to service disruptions as well as failures to provide adequate support for reasons that are outside of our direct control. We have experienced, and expect that in the future we may experience interruptions, delays and outages in service and availability from time to time due to a variety of factors, including infrastructure changes, human or software errors, website hosting disruptions and capacity constraints.

The following factors, many of which are beyond our control, can affect the delivery, availability, and the performance of our Falcon platform. . . .

- failure by us to maintain and update our cloud infrastructure to meet our data capacity requirements;
- errors, defects or performance problems in our software, including third-party software incorporated in our software;
- improper deployment or configuration of our solutions;

- the failure of our redundancy systems, in the event of a service disruption at one of our data centers, to provide failover to other data centers in our data center network; and
- the failure of our disaster recovery and business continuity arrangements.

The adverse effects of any service interruptions on our reputation, results of operations, and financial condition may be disproportionately heightened due to the nature of our business and the fact that our customers have a low tolerance for interruptions of any duration. Interruptions or failures in our service delivery could result in a cyberattack or other security threat to one of our customers during such periods of interruption or failure. Additionally, interruptions or failures in our service could cause customers to terminate their subscriptions with us, adversely affect our renewal rates, and harm our ability to attract new customers. Our business would also be harmed if our customers believe that a cloud-based SaaS-delivered endpoint security solution is unreliable. While we do not consider them to have been material, we have experienced, and may in the future experience, service interruptions and other performance problems due to a variety of factors. The occurrence of any of these factors, or if we are unable to rapidly and cost-effectively fix such errors or other problems that may be identified, could damage our reputation, negatively affect our relationship with our customers or otherwise harm our business, results of operations and financial condition.

84. The 2024 10-K was signed by Defendants Kurtz, Podbere, Watzinger, Davis, O’Leary, Sullivan, Flower, Schumacher, Austin, and Gandhi. The 2024 10-K was also accompanied by SOX Certifications made by Defendants Kurtz and Podbere. In the SOX Certifications, Defendants Kurtz and Podbere attested to the accuracy of the 2024 10-K.

85. Also on March 7, 2024, Defendant Kurtz attended the Morgan Stanley Technology, Media & Telecom Conference on behalf of CrowdStrike. When asked about deploying CrowdStrike’s new products, Defendant Kurtz stated, in relevant part, that it is “friction-free to deploy [the Company’s] product.”

86. On May 6, 2024, CrowdStrike filed a Proxy Statement on a Schedule 14A with the SEC (the “2024 Proxy”). In the 2024 Proxy, the Company touted its risk oversight policies and mechanisms, stating, in relevant part:

Risk is inherent with every business, and we face a number of risks, including strategic, financial, business and operational, cybersecurity, legal and compliance, and reputational risks, in the pursuit and achievement of our strategic objectives. We have designed and implemented processes to manage risk in our operations. Management is responsible for the day-to-day oversight and management of strategic, operational, legal and compliance, cybersecurity, and financial risks, while our Board, as a whole and assisted by its committees, has responsibility for the oversight of our risk management framework, which is designed to identify, assess, and manage risks to which our Company is exposed, as well as foster a corporate culture of integrity. Consistent with this approach, our Board regularly reviews our strategic and operational risks in the context of discussions with management, question and answer sessions, and reports from the management team at each regular board meeting. Our Board also receives regular reports on all significant committee activities at each regular board meeting and evaluates the risks inherent in significant transactions.

In addition, our Board has tasked designated standing committees with oversight of certain categories of risk management. Our Audit Committee assists our Board in fulfilling its oversight responsibilities with respect to risk assessment and risk management, including the Company's policies and practices pertaining to financial accounting, investment, tax, and cybersecurity matters, and discusses with management the Company's major financial risk exposures. Our Compensation Committee reviews and assesses risks arising from the Company's employee compensation policies and practices and whether any such risks are reasonably likely to have a material adverse effect on the Company. Our Nominating and Corporate Governance Committee monitors the effectiveness of our corporate governance guidelines and policies. Our Transaction Committee reviews and evaluates certain risks related to potential acquisitions of businesses, entities or technologies.

Our Board believes its current leadership structure supports the risk oversight function of the Board.

87. On June 5, 2024, the Company filed its quarterly report for the period ended April 30, 2024 with the SEC (the "Q1 2025 10-Q"). The Q1 2025 10-Q again discussed the potential risks to the Falcon platform, stating, in relevant part:

We rely on third-party data centers, such as Amazon Web Services, and our own colocation data centers to host and operate our Falcon platform, and any disruption of or interference with our use of these facilities may negatively affect our ability to maintain the performance and reliability of our Falcon platform which could cause our business to suffer.

Our customers depend on the continuous availability of our Falcon platform. We currently host our Falcon platform and serve our customers using a mix of third-party data centers, primarily Amazon Web Services, Inc., or AWS, and our data centers, hosted in colocation facilities. Consequently, we may be subject to service disruptions as well as failures to provide adequate support for reasons that are outside of our direct control. We have experienced, and expect that in the future we may experience interruptions, delays and outages in service and availability from time to time due to a variety of factors, including infrastructure changes, human or software errors, website hosting disruptions and capacity constraints.

The following factors, many of which are beyond our control, can affect the delivery, availability, and the performance of our Falcon platform. . . .

- failure by us to maintain and update our cloud infrastructure to meet our data capacity requirements;
- errors, defects or performance problems in our software, including third-party software incorporated in our software;
- improper deployment or configuration of our solutions;
- the failure of our redundancy systems, in the event of a service disruption at one of our data centers, to provide failover to other data centers in our data center network; and
- the failure of our disaster recovery and business continuity arrangements.

The adverse effects of any service interruptions on our reputation, results of operations, and financial condition may be disproportionately heightened due to the nature of our business and the fact that our customers have a low tolerance for interruptions of any duration. Interruptions or failures in our service delivery could result in a cyberattack or other security threat to one of our customers during such periods of interruption or failure. Additionally, interruptions or failures in our service could cause customers to terminate their subscriptions with us, adversely affect our renewal rates, and harm our ability to attract new customers. Our business would also be harmed if our customers believe that a cloud-based SaaS-delivered endpoint security solution is unreliable. While we do not consider them to have been material, we have experienced, and may in the future experience, service interruptions and other performance problems due to a variety of factors. The occurrence of any of these factors, or if we are unable to rapidly and cost-effectively fix such errors or other problems that may be identified, could damage our reputation, negatively affect our relationship with our customers or otherwise harm our business, results of operations and financial condition.

88. The Q1 2025 10-Q was accompanied by SOX Certifications made by Defendants Kurtz and Podbere. In the SOX Certifications, Defendants Kurtz and Podbere attested to the accuracy of the Q1 2025 10-Q.

89. The above statements were materially false and/or misleading and failed to disclose material adverse facts about the Company's business, operations, and prospects. Specifically, the Individual Defendants failed to disclose to investors that: (i) the Company had insufficient controls in place for its procedures used to update Falcon; (ii) the Company was not properly testing updates to the Falcon platform before rolling the updates out to CrowdStrike's customer base; (iii) the inadequate software testing created a substantial risk that an update to the Falcon platform could result in widespread outages; (iv) any such outages caused by the updates would cause substantial reputational harm and legal risk to the Company; and (v) as a result of the foregoing, Defendants' positive statements about the Company's business, operations, and prospects were materially misleading and/or lacked a reasonable basis.

The Truth is Revealed

90. The truth began to emerge on July 19, 2024, when it was revealed that, as a result of the update to CrowdStrike's Falcon platform, there were widespread technology outages that affected millions of users of Microsoft Windows systems worldwide. The outage impacted approximately 8.5 million devices worldwide.²³

91. On the news of the outage, the Company's stock price fell \$38.09 per share, or approximately 11.1%, to close at \$304.96 per share on July 19, 2024.

92. The truth continued to emerge on July 22, 2024, when it was revealed that Defendant Kurtz was contacted by Congress to testify regarding the CrowdStrike outage. In a letter

²³ Fung, *supra* note 2.

to Defendant Kurtz, the congressional panel stated, in relevant part “[w]hile we appreciate CrowdStrike’s response and coordination with stakeholders, we cannot ignore the magnitude of this incident, which some have claimed is the largest IT outage in history.”²⁴

93. Also on July 22, 2024, analysts, including Guggenheim Securities and BTIG, downgraded CrowdStrike’s stock rating. Both Guggenheim and BTIG downgraded their ratings of the Company’s stock from “buy” to “neutral.”²⁵

94. Furthermore, on July 22, 2024, *Forbes* published an article revealing that the devastating effects that the CrowdStrike outage caused were continuing to plague many airlines, mainly Delta Air Lines. The *Forbes* article stated, in relevant part:

Delta Air Lines, in particular, is the U.S. carrier still experiencing the most harmful effects from the outage. As of the morning of July 22, FlightAware reports the airline has over 700 cancellations and 400 flight delays that will increase as the day progresses.

By comparison, American Airlines, United Airlines, Alaska Airlines, Frontier Airlines and Southwest Airlines each have 40 cancellations or fewer over the same period.

Clearly, Delta has the most applications linked to the affected Microsoft Windows operating system. Experts are resolving the malfunction, although the process is tedious as it can require rebooting of computer systems at each airport gate across its system. The airline canceled more than 4,800 flights over the first three days and experienced numerous delays.²⁶

95. On this news of the aftermath of the outage, the Company’s stock price fell \$41.05 per share, or approximately 13.46%, to close at \$263.91 per share on July 22, 2024.

96. Then, on July 29, 2024, the truth fully emerged when it was revealed that the effects from the outage on the Company were far from over, with news breaking that Delta retained a prominent attorney, David Boies, to pursue potential damages from CrowdStrike and Microsoft

²⁴ Singh, *supra* note 3.

²⁵ Novet, *supra* note 4; Maybach, *supra* note 4.

²⁶ Whitmore, *supra* note 5.

for the outage.²⁷

97. On this news, the Company's stock price fell \$25.16 per share, or approximately 9.72%, to close at \$233.65 per share on July 30, 2024.

Insider Sales

98. During the Relevant Period, Defendants Sentonas, Podbere, Kurtz, Gandhi, O'Leary, and Austin made sales of the Company's stock while in possession of material non-public information concerning the Company's financial condition and internal controls.

99. While the Company's stock price was artificially inflated during the Relevant Period, Defendant Sentonas sold 88,578 shares of Company stock, totaling proceeds of approximately \$25.4 million. Sentonas made the following sales of CrowdStrike stock during the Relevant Period:

Date	Number of Shares Sold	Average Price Per Share	Proceeds
11/30/2023	26,652	\$236.00	\$6,289,872
12/21/2023	10,321	\$254.75	\$2,621,534
1/16/2024	22,123	\$286.00	\$6,327,178
3/21/2024	18,747	\$325.80	\$6,107,772.60
6/21/2024	10,735	\$380.63	\$4,086,063.05

100. While the Company's stock price was artificially inflated during the Relevant Period, Defendant Podbere sold approximately 217,069 shares of Company stock, totaling proceeds of approximately \$66.1 million. Podbere made the following sales of CrowdStrike stock during the Relevant Period:

Date	Number of Shares Sold	Average Price Per Share	Proceeds
12/12/2023	30,000	\$250.04	\$7,501,200
12/21/2023	22,825	\$253.22	\$5,779,746.50
3/21/2024	26,097	\$325.61	\$8,497,444.17
4/1/2024	64,000	\$316.48	\$20,254,720

²⁷ Novet & Levy, *supra* note 6.

5/3/2024	15,753	\$305.15	\$4,807,027.95
5/14/2024	12,000	\$329.10	\$3,949,200
5/15/2024	12,000	\$339.29	\$4,071,503
5/20/2024	5,424	\$349.01	\$1,893,030.24
5/21/2024	6,576	\$348.94	\$2,294,629
6/21/2024	11,154	\$379.81	\$4,236,400.74

101. While the Company's stock price was artificially inflated during the Relevant Period, Defendant Kurtz sold approximately 346,931 shares of Company stock, totaling proceeds of approximately \$106.5 million. Kurtz made the following sales of CrowdStrike stock during the Relevant Period:

Date	Number of Shares Sold	Average Price Per Share	Proceeds
12/21/2023	56,985	\$252.15	\$14,368,767.80
1/11/2024	60,000	\$283.69	\$17,201,400
1/12/2024	40,000	\$286.10	\$11,444,000
3/21/2024	78,080	\$326.78	\$25,514,982.40
5/3/2024	56,279	\$304.41	\$17,131,890.40
6/21/2024	55,587	\$376.45	\$20,925,762.20

102. While the Company's stock price was artificially inflated during the Relevant Period, Defendant Gandhi sold approximately 45,000 shares of Company stock, totaling proceeds of approximately \$14 million. Gandhi made the following sales of CrowdStrike stock during the Relevant Period:

Date	Number of Shares Sold	Average Price Per Share	Proceeds
1/3/2024	15,000	\$240.13	\$3,601,950
4/3/2024	15,000	\$316.82	\$4,752,300
7/1/2024	15,000	\$380.21	\$5,703,150

103. While the Company's stock price was artificially inflated during the Relevant Period, Defendant O'Leary sold approximately 9,340 shares of Company stock, totaling proceeds of approximately \$1.1 million. O'Leary made the following sales of CrowdStrike stock during the Relevant Period:

Date	Number of Shares Sold	Average Price Per Share	Proceeds
12/7/2023	4,040	\$238.32	\$962,812.80
6/10/2024	5,300	\$381.45	\$2,021,685

104. While the Company's stock price was artificially inflated during the Relevant Period, Defendant Austin sold 15,000 shares of Company stock, totaling proceeds of approximately \$5.85 million. Austin made the following sales of CrowdStrike stock during the Relevant Period:

Date	Number of Shares Sold	Average Price Per Share	Proceeds
6/27/2024	10,000	\$390.01	\$3,900,100
6/28/2024	5,000	\$391.01	\$1,955,050

105. As a result of these insider sales, Defendants Sentonas, Podbere, Kurtz, Gandhi, O'Leary, and Austin were unjustly enriched.

Harm to the Company

106. As a direct and proximate result of the Individual Defendants' misconduct, CrowdStrike has lost and expended, and will lose and expend, millions of dollars.

107. Such expenditures include, but are not limited to, the legal fees associated with the Securities Class Action filed against the Company and Defendants Kurtz and Podbere, the legal fees associated with the Consumer Class Actions filed against the Company, and amounts paid to outside lawyers, accountants, and investigators in connection therewith.

108. Such expenditures also include, but are not limited to, significant compensation and benefits paid to the Individual Defendants who breached their fiduciary duties to the Company.

109. Furthermore, the Securities Class Action and the Consumer Class Actions have exposed the Company to massive class-wide liability.

DERIVATIVE AND DEMAND FUTILITY ALLEGATIONS

110. Plaintiff brings this action derivatively in the right and for the benefit of the Company to redress injuries suffered and to be suffered as a direct and proximate result of the breaches of fiduciary duties by the Individual Defendants.

111. Plaintiff will adequately and fairly represent the interests of CrowdStrike and its shareholders in enforcing and prosecuting its rights.

112. CrowdStrike is named solely as a nominal party in this action. This is not a collusive action to confer jurisdiction on this Court that it would otherwise not have.

113. Plaintiff is a current shareholder of CrowdStrike and was a continuous shareholder of the Company during the period of the Individual Defendants' wrongdoing alleged herein. Plaintiff will adequately and fairly represent the interests of the Company in enforcing and prosecuting its rights and retained counsel competent and experienced in derivative litigation.

114. A pre-suit demand on the Board of CrowdStrike is futile and, therefore, excused. At the time this action was commenced, the nine-person Board consisted of Individual Defendants Watzinger, Kurtz, Austin, Davis, Flower, Gandhi, O'Leary, Schumacher, and Sullivan (the "Director Defendants"). As set forth below, all of the Director Defendants are incapable of making an independent and disinterested decision to institute and vigorously prosecute this action because they face a substantial likelihood of liability for the misconduct alleged herein. Therefore, demand on the Board to institute this action is not necessary because such a demand would have been a futile and useless act.

115. The Director Defendants either knew or should have known of the false and misleading statements that were issued on the Company's behalf and took no steps in a good faith effort to prevent or remedy that situation.

116. Each of the Director Defendants approved and/or permitted the wrongs alleged

herein to have occurred and participated in efforts to conceal or disguise those wrongs from the Company's stockholders or recklessly and/or with gross negligence disregarded the wrongs complained of herein and are therefore not disinterested parties.

117. Each of the Individual Defendants authorized and/or permitted the false statements to be disseminated directly to the public and made available and distributed to shareholders, authorized and/or permitted the issuance of various false and misleading statements, and are principal beneficiaries of the wrongdoing alleged herein, and thus, could not fairly and fully prosecute such a suit even if they instituted it.

118. As members of the Board charged with overseeing the Company's affairs, each of the Director Defendants had knowledge, or the fiduciary obligation to inform themselves, of information pertaining to the Company's core operations and the material events giving rise to these claims. Specifically, as Board members of CrowdStrike, the Director Defendants knew, or should have known, the material facts surrounding CrowdStrike's financial condition and internal control mechanisms.

119. Defendant Kurtz is not disinterested or independent. Defendant Kurtz is co-founder of the Company and serves as Chairman of the Board and as the Company's CEO and President. Thus, the Company admits that Defendant Kurtz is a non-independent director.

120. Furthermore, in the 2024 Proxy, the Company conceded that Defendant Flower is not an independent director due to Defendant Flower's previous employment as Chief Marketing Officer of the Company. Thus, the Company admits that Defendant Flower is a non-independent director.

121. Moreover, Director Defendants Watzinger, Kurtz, Austin, Davis, Flower, Gandhi, O'Leary, Schumacher, and Sullivan signed the 2024 10-K. Defendant Kurtz also signed SOX

Certifications that accompanied the Q3 2024 10-Q, 2024 10-K, and Q1 2025 10-Q. Accordingly, these Director Defendants breached their fiduciary duties, face a substantial likelihood of liability, are not independent or disinterested, and thus demand upon them is futile, and, therefore, excused.

122. Additionally, each of the Director Defendants received payments, benefits, stock options, and other emoluments by virtue of their membership on the Board and their control of the Company.

123. Moreover, the Director Defendants willfully ignored, or recklessly failed to inform themselves of, the obvious problems with the Company's internal controls, practices, and procedures and failed to make a good faith effort to correct the problems or prevent their recurrence. As a result of the foregoing, the Director Defendants breached their fiduciary duties, face a substantial likelihood of liability, are not disinterested, and demand upon them is futile, and thus excused.

124. Additionally, the Director Defendants took no action to redress the harm suffered by the Company resulting from the misconduct alleged herein.

125. Defendants Watzinger, Austin, and Sullivan (the "Audit Defendants") serve on the Company's Audit Committee, and pursuant to the Audit Committee Charter, were specifically charged with the responsibility to assist the Board in fulfilling its oversight responsibilities related to, *inter alia*, financial reporting and the underlying internal controls and procedures over financial reporting. At all relevant times, however, the Audit Defendants breached their fiduciary duty to the Company by failing to prevent, correct, or inform the Board of the issuance of material misstatements and omissions regarding the Company's business, finances, and operations, as alleged above. Therefore, the Audit Defendants cannot independently consider any demand to sue themselves for breaching their fiduciary duties to the Company, as that would expose them to

substantial liability and threaten their livelihoods.

126. The Director Defendants, as members of the Board, were and are subject to the Company's Code of Conduct. The Code of Conduct goes well beyond the basic fiduciary duties required by applicable laws, rules, and regulations, requiring the Director Defendants to also adhere to the Company's standards of business conduct. The Director Defendants violated the Code of Conduct because they knowingly or recklessly participated in making and/or causing the Company to make the materially false and misleading statements alleged herein. Because the Director Defendants violated the Code of Conduct, they face a substantial likelihood of liability for breaching their fiduciary duties, and therefore demand upon them is futile.

127. Accordingly, a pre-suit demand on the Board is futile and excused.

COUNT I

Against the Individual Defendants for Violations of § 10(b) of the Exchange Act and Rule 10b-5

128. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

129. The Individual Defendants violated § 10(b) of the Exchange Act, 15 U.S.C. § 78j(b), and Rule 10b-5 promulgated thereunder by the SEC.

130. The Individual Defendants, individually and in concert, directly or indirectly, disseminated or approved the false statements specified above, which they knew or deliberately disregarded were misleading in that they contained misrepresentations and failed to disclose material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading.

131. The Individual Defendants violated §10(b) of the Exchange Act and Rule 10b-5 in that they: (i) employed devices, schemes and artifices to defraud; (ii) made untrue statements of

material facts or omitted to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; or (iii) engaged in acts, practices and a course of business that operated as a fraud or deceit upon Plaintiff and others similarly situated.

132. The Individual Defendants acted with scienter because they (i) knew that the public documents and statements issued or disseminated in the name of CrowdStrike were materially false and misleading; (ii) knew that such statements or documents would be issued or disseminated to the investing public; and (iii) knowingly and substantially participated or acquiesced in the issuance or dissemination of such statements or documents as primary violations of the securities laws.

133. The Individual Defendants, by virtue of their receipt of information reflecting the true facts of CrowdStrike, their control over, and/or receipt and/or modification of CrowdStrike's allegedly materially misleading statements, and/or their associations with the Company which made them privy to confidential proprietary information concerning CrowdStrike, participated in the fraudulent scheme alleged herein.

134. As a result of the foregoing, the market price of CrowdStrike common stock was artificially inflated. In ignorance of the falsity of the statements, stockholders relied on the statements described above and/or the integrity of the market price of CrowdStrike common stock in purchasing CrowdStrike common stock at prices that were artificially inflated as a result of these false and misleading statements and were damaged thereby.

135. In addition, as a result of the wrongful conduct alleged herein, the Company has suffered significant damages, including the costs and expenses incurred in defending itself in the Securities Action and reputational harm. The Individual Defendants, through their violation of

Section 10(b) of the Exchange Act, 15 U.S.C. § 78j(b), and Rule 10b-5, have exposed the Company to millions of dollars in potential class-wide damages in the Securities Class Action.

COUNT II

Against the Individual Defendants For Breach of Fiduciary Duty

136. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

137. The Individual Defendants owed the Company fiduciary obligations. By reason of their fiduciary relationships, the Individual Defendants owed the Company the highest obligation of good faith, fair dealing, loyalty, and due care.

138. Each of the Individual Defendants violated and breached their fiduciary duties of care, loyalty, reasonable inquiry, good faith, loyalty, oversight, and supervision.

139. The Individual Defendants engaged in a sustained and systematic failure to properly exercise their fiduciary duties. Among other things, the Individual Defendants breached their fiduciary duties of loyalty and good faith by permitting the use of inadequate practices and procedures to guide the truthful dissemination of Company news to the investing public and to the Company's shareholders, allowing or permitting false and misleading statements to be disseminated in the Company's SEC filings and other disclosures, and otherwise failing to ensure that adequate internal controls were in place regarding the serious business reporting issues and deficiencies described above. These actions could not have been a good faith exercise of prudent business judgment to protect and promote the Company's corporate interests.

140. Specifically, the Individual Defendants willfully or recklessly made and/or caused the Company to make false and/or misleading statements and omissions of material fact that failed to disclose, *inter alia*, that: (i) the Company had insufficient controls in place for its procedures

used to update Falcon; (ii) the Company was not properly testing updates to the Falcon platform before rolling the updates out to CrowdStrike's customers; (iii) the inadequate software testing created a substantial risk that an update to the Falcon platform could result in widespread outages; (iv) any such outages caused by the updates would cause substantial reputational harm and legal risk to the Company; and (v) as a result of the foregoing, Defendants' positive statements about the Company's business, operations, and prospects were materially misleading and/or lacked a reasonable basis.

141. The Individual Defendants had actual knowledge that the Company was engaging in the fraudulent scheme set forth herein, and that internal controls were not adequately maintained, or acted with reckless disregard for the truth, in that they caused the Company to improperly engage in the fraudulent scheme and to fail to maintain adequate internal controls, even though such facts were available to them. The Individual Defendants, in good faith, should have taken appropriate action to correct the scheme alleged herein and to prevent it from continuing to occur.

142. In further breach of their fiduciary duties, the Individual Defendants failed to correct and/or caused the Company to fail to correct the false and/or misleading statements and omissions of material fact referenced herein.

143. As a direct and proximate result of the Individual Defendants' failure to fulfill their fiduciary obligations, the Company has sustained significant damages.

144. As a result of the misconduct alleged herein, the Individual Defendants are liable to the Company. As a direct and proximate result of the Individual Defendants' breach of their fiduciary duties, the Company has suffered damage, not only monetarily, but also to its corporate image and goodwill. Such damage includes, among other things, costs incurred in defending itself in the Securities Class Action and the Consumer Class Actions, exposing the Company to millions

of dollars in potential class-wide damages in the Securities Class Action and Consumer Class Actions, and damage to the share price of the Company's stock, resulting in an increased cost of capital, and reputational harm.

145. Plaintiff, on behalf of CrowdStrike, has no adequate remedy at law.

COUNT III

Against the Individual Defendants for Aiding and Abetting Breach of Fiduciary Duty

146. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

147. By encouraging and accomplishing the illegal and improper transactions alleged herein and concealing them from the public, the Individual Defendants have each encouraged, facilitated, and advanced their breaches of their fiduciary duties. In so doing, the Individual Defendants have each aided and abetted, conspired, and schemed with one another to breach their fiduciary duties, waste the Company's corporate assets, and engage in the ultra vires and illegal conduct complained of herein.

148. Plaintiff on behalf of CrowdStrike has no adequate remedy at law.

COUNT IV

Against the Individual Defendants for Unjust Enrichment

149. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

150. By their wrongful acts, violations of law, and false and misleading statements and omissions of material fact that they made and/or caused to be made, the Individual Defendants were unjustly enriched at the expense of, and to the detriment of, CrowdStrike.

151. The Individual Defendants either benefitted financially from the improper conduct, or received bonuses, stock options, or similar compensation from CrowdStrike that was tied to the performance or artificially inflated valuation of CrowdStrike, or received compensation that was unjust in light of the Individual Defendants' bad faith conduct.

152. Plaintiff, as a shareholder and a representative of CrowdStrike, seeks restitution from the Individual Defendants and seeks an order from this Court disgorging all profits, benefits and other compensation procured by the Individual Defendants due to their wrongful conduct and breach of their fiduciary and contractual duties.

153. Plaintiff on behalf of CrowdStrike has no adequate remedy at law.

COUNT V

Against the Individual Defendants for Waste of Corporate Assets

154. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

155. The wrongful conduct alleged regarding the issuance of false and misleading statements was continuous, connected, and on-going throughout the time period in issue. It resulted in continuous, connected, and ongoing harm to the Company.

156. As a result of the misconduct described above, the Individual Defendants wasted corporate assets by, *inter alia*: (i) paying and collecting excessive compensation and bonuses; and (ii) incurring potentially millions of dollars of legal liability and/or legal costs, including defending against the Securities Class Action and the Consumer Class Actions.

157. As a result of the waste of corporate assets, the Individual Defendants are liable to the Company.

158. Plaintiff on behalf CrowdStrike has no adequate remedy at law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff demands judgment as follows:

- A. Awarding money damages against all Individual Defendants, jointly and severally, for all losses and damages suffered as a result of the acts and transactions complained of herein, together with pre-judgment interest, molded in a fashion to ensure the Individual Defendants do not participate therein or benefit thereby;
- B. Directing all Individual Defendants to account for all damages caused by them and all profits and special benefits and unjust enrichment they have obtained as a result of their unlawful conduct, including all salaries, bonuses, fees, stock awards, options and common stock sale proceeds, and imposing a constructive trust thereon;
- C. Awarding punitive damages;
- D. Awarding costs and disbursements of this action, including reasonable attorneys' fees, accountants' and experts' fees, costs, and expenses; and
- E. Granting such other and further relief as the Court deems just and proper.

JURY DEMAND

Plaintiff hereby demands a trial by jury on all claims set forth herein.

DATED: September 19, 2024

THE BRISCOE LAW FIRM, P.C.

By: /s/ Willie C. Briscoe
Willie C. Briscoe
Texas Bar No. 24001788
12700 Park Central Drive, Suite 520
Dallas, TX 75251
Telephone: (972) 521-6868
Facsimile: (346) 214-7463
Email: wbriscoe@briscoelawfirm.com

OF COUNSEL:

RIGRODSKY LAW, P.A.

Seth D. Rigrotsky

Timothy J. MacFall

Gina M. Serra

Vincent A. Licata

825 East Gate Boulevard, Suite 300

Garden City, NY 11530

Telephone: (516) 683-3516

Email: sdr@rl-legal.com

tjm@rl-legal.com

gms@rl-legal.com

vl@rl-legal.com

GRABAR LAW OFFICE

Joshua H. Grabar

One Liberty Place

1650 Market Street, Suite 3600

Philadelphia, PA 19103

Telephone: (267) 507-6085

Email: jgrabar@grabarlaw.com

VERIFICATION

I, Nathan Silva, have reviewed the allegations made in the Verified Shareholder Derivative Complaint, know the contents thereof, and authorize its filing. To those allegations of which I have personal knowledge, I believe those allegations to be true. As to those allegations of which I do not have personal knowledge, I rely upon my counsel and their investigation and believe them to be true. I further declare that I am a current holder, and have been a holder, of CrowdStrike Holdings, Inc. common stock at all relevant times.

I declare under penalty of perjury under the laws of the United States that the foregoing is
9/18/2024
true and correct. Executed this ____ day of ____ 2024.

DocuSigned by:
Nathan Silva
C3263758AD4944B...
Nathan Silva